LATHAM & WATKINS LLP
Elizabeth L. Deeley (Bar No. 230798)
elizabeth.deeley@lw.com
Sheridan Caldwell (Bar No. 324743)
sheridan.caldwell@lw.com
505 Montgomery Street, Suite 2000
San Francisco, California 94111-6538
Telephone: +1.415.391.0600

Serrin Turner (*pro hac vice*)
serrin.turner@lw.com
Marissa Alter-Nelson (*pro hac vice*)
marissa.alter-nelson@lw.com
1271 Avenue of the Americas
New York, New York 10022-4834
Telephone: +1.212.906.1200

Attorneys for Defendant Meta Platforms, Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

In re Meta Browser Tracking Litigation	Case No. 4:22-cv-05267-JST
	DEFENDANT META PLATFORMS, INC.'S NOTICE OF MOTION AND MOTION TO DISMISS CONSOLIDATED CLASS ACTION COMPLAINT Date: June 22, 2023 Time: 2:00 p.m. Court: Courtroom 6—2nd Floor Judge: Hon. Jon S. Tigar

NOTICE OF MOTION AND MOTION TO DISMISS

TO PLAINTIFFS AND TO THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on June 22, 2023, at 2:00 p.m. in Courtroom 6 of the United States District Court for the Northern District of California, located at 1301 Clay Street, Oakland, California, Defendant Meta Platforms, Inc., will and hereby does move for an order dismissing Plaintiffs' Consolidated Class Action Complaint (Dkt. 36, "Complaint").

This motion is made pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6), on the grounds that Plaintiffs lack Article III standing to bring any claim, and each of the causes of action in the Complaint fails to state a claim as a matter of law.

This motion is based on this Notice of Motion and Motion to Dismiss, the Memorandum of Points and Authorities, Defendant's Request for Judicial Notice, the Declaration of Serrin Turner, the pleadings and papers on file in this action, the arguments of counsel, and any other matter that the Court may properly consider.

STATEMENT OF RELIEF SOUGHT

Meta seeks an order pursuant to Federal Rule of Civil Procedure 12(b)(1) and 12(b)(6) dismissing this action for lack of Article III standing and failure to state a claim upon which relief can be granted.

DATED: March 23, 2023

LATHAM & WATKINS LLP

By: /s/ *Serrin Turner*
Elizabeth L. Deeley (Bar No. 230798)
elizabeth.deeley@lw.com
Sheridan Caldwell (Bar No. 324743)
sheridan.caldwell@lw.com
505 Montgomery Street, Suite 2000
San Francisco, CA 94111-6538
Telephone: +1.415.391.0600

Serrin Turner (*pro hac vice*)
serrin.turner@lw.com
Marissa Alter-Nelson (*pro hac vice*)
marissa.alter-nelson@lw.com
1271 Avenue of the Americas
New York, New York 10022-4834
Telephone: +1.212.906.1200

Attorneys for Defendant Meta Platforms, Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

RULES

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Plaintiffs rushed into court to file this litigation after seeing a blog post critical of Meta Platforms, Inc. ("Meta")—without closely reading, or else deliberately ignoring, what it actually says. The blog post concerns the in-app web browser included as part of Meta's Facebook and Instagram apps—i.e., a browsing window that opens within Facebook or Instagram when a user clicks on a link within the app to a third-party site (the "In-App Browser"). Relying exclusively on the blog post, Plaintiffs allege that Meta surreptitiously monitors and records everything that users do in the In-App Browser—"down to the keystroke," Compl. ¶ 2[1]—even if they have opted out of "tracking" on their iPhones under Apple's App Tracking Transparency ("ATT") policy. (The ATT policy requires iPhone apps to ask users for permission before "tracking" their activity across third-party websites for advertising-related purposes.) The entire Complaint is based on this theory.

The problem for Plaintiffs, however, is that the blog post they rely on actually *contradicts* their core allegations. While the blog post criticizes the use of in-app browsers, based on the concern that app developers *could* use such browsers to improperly collect user browsing activity, it never asserts that Meta *actually* uses its In-App Browser in such a way. To the contrary, the blog post expressly *disavows* any claim that Meta engages in the type of indiscriminate data collection Plaintiffs allege, and it specifically *affirms* that Meta is complying with Apple's ATT policy.

Under the incorporation by reference doctrine, where Plaintiffs selectively rely on portions of a document to support their claims, but omit other portions that contradict them, the Court need not credit the contradicted allegations as true. Here, when the allegations contradicted by the blog post are removed, the Complaint has no other leg to stand on: there is no plausible alternative factual basis asserted in the Complaint that could support Plaintiffs' otherwise conclusory claims that Meta monitors and records all of their actions in the In-App Browser without their consent.

[1] References herein to "the Complaint" or "Compl." refer to the Consolidated Class Action Complaint, Dkt. 36.

All that remains is speculation that Meta could theoretically use the In-App Browser to do so. That speculation is not enough to establish standing to sue Meta, let alone plausibly plead any of Plaintiffs' causes of action. The Court should reject Plaintiffs' effort to concoct a basis for a lawsuit by pointing to a document as the factual source for their claims while inaccurately portraying its contents. All of Plaintiffs claims should be dismissed on this ground alone.

Beyond this fundamental flaw that cuts across all of their claims, several of Plaintiffs' claims fail for additional, claim-specific reasons. First, their claim under the federal computer hacking statute, the Computer Fraud and Abuse Act ("CFAA"), fails because Plaintiffs do not allege any conduct constituting computer hacking, nor do they allege any loss or damage cognizable under the statute. Second, their equitable claims are barred under Ninth Circuit precedent because they have not, and cannot, plead that legal relief would be insufficient to remedy any of their alleged harms—even if any such harms actually existed. Third, their claim under the California Unfair Competition Law ("UCL") fails not only because it is equitable in nature but also because Plaintiffs lack statutory standing under the UCL, as they have not validly alleged any loss of money or property.

For all of these reasons, as detailed below, the Complaint should be dismissed in its entirety.

II. BACKGROUND

A. The Blog Post Cited as the Source for Plaintiffs' Core Claims

On August 10, 2022, a self-described security researcher named Felix Krause published a post on his blog site, entitled "*iOS Privacy: Instagram and Facebook can track anything you do on any website in their in-app browser*" ("Krause Post"). *See* Ex. 1 at 1.[2] The Krause Post concerns the In-App Browser used on Meta's Facebook and Instagram apps for iOS (Apple's mobile operating system for iPhones). *Id.* at 1-2. As alleged in the Complaint, the In-App Browser is a custom browser window built into the Facebook and Instagram apps that automatically opens when a user clicks on a link to a third-party website while using the app (such as a link to a news story

[2] All exhibits cited herein are attached to the Declaration of Serrin Turner, filed herewith.

forwarded by a friend on Facebook or a link to a product featured in an ad displayed in the app). Compl. ¶ 5.

The underlying premise of the Krause Post is that "using a custom in-app browser . . . causes various risks for the user," in that "the host app [is] able to track every single interaction with external websites, from all form inputs like passwords and addresses, to every single tap." Ex. 1 at 1. The underlined text links to a further post by Krause, where he explains that a custom in-app browser can run JavaScript code (a type of computer code that can run in a web browser) created by the app developer, which Krause worries *could* be used by the app developer for *any* purpose. Ex. 2 at 2-3. As Krause states: "Using a custom in-app browser, allows the app developer to inject ANY JavaScript code into the website the user visits. This means, any content, any data and any input that is shown or stored on the website is accessible to the app." Ex. 2 at 3.

On this basis, and with little consideration of the potential benefits of using a custom in-app browser,[3] the Krause Post criticizes Meta for using a custom in-app browser in its apps, as opposed to relying on the default browser on a user's iOS device. Ex. 1 at 1, 4. Yet, notwithstanding this criticism, the Krause Post repeatedly disavows any allegation that Meta *actually* uses the In-App Browser to collect data for an improper purpose. As the Krause Post states:

> The Instagram[4] app injects their JavaScript code into every website shown, including when clicking on ads. *Even though the injected script doesn't currently do this*, running custom scripts on third party websites allows them to monitor all user interactions, like every button & link tapped, text selections, screenshots, as well as any form inputs, like passwords, addresses and credit card numbers.

Id. at 1-2 (emphasis added). Similarly, in a section of the Krause Post labeled "FAQs for Non-Tech Readers," Krause states:

[3] While not necessary to consider for purposes of this motion, the benefits of the In-App Browser are explained on Meta's website. *See* Meta Business Help Center, *About the in-app browser for Facebook and Instagram*, https://www.facebook.com/business/help/206578174518231 (explaining that the in-app browser provides both convenience and safety features for users).

[4] The Krause Post states that, for simplicity, it refers to "Instagram" throughout, even though its statements are meant to apply to Facebook as well. *See id.* at 1 ("To keep this post simple, I'll use 'Instagram' instead of 'Meta' or 'Facebook.'").

> **Does Facebook actually steal my passwords, address and credit card numbers?** No! I didn't prove the exact data Instagram is tracking, but wanted to showcase the kind of data they could get without you knowing. As shown in the past, if it's possible for a company to get access to data legally and for free, without asking the user for permission, they will track it.

Id. at 3 (emphasis in original). In other words, while Krause expresses concern that the In-App Browser adds certain JavaScript to the web pages it displays and that JavaScript *in theory* can be used to collect any data from a user, he disclaims any knowledge of what specific data Meta actually collects through the JavaScript included in the In-App Browser, or what Meta actually does with any data that may be collected.

The Krause Post also notes a concern that JavaScript code on an in-app browser theoretically *could* be used to circumvent Apple's ATT policy—but he specifically clarifies that Meta does *not actually* do so with the In-App Browser. *Id.* at 2-4. The ATT policy, as described by Plaintiffs, was first introduced in an iOS update in April 2021, and "require[s] app developers, like Meta, to obtain users' express consent before tracking their activity on third-party websites for the purposes of advertising or sharing the information with data brokers." Compl. ¶ 4. Apple states the policy more precisely in explaining it to users:

> In iOS 14.5, iPadOS 14.5, and tvOS 14.5, or later, apps must ask for permission before tracking your activity across other companies' apps and websites. Tracking occurs when information that identifies you or your device collected from an app is linked with information that identifies you or your device collected on apps, websites and other locations owned by third parties for the purposes of targeted advertising or advertising measurement, or when the information collected is shared with data brokers.

Ex. 3 at 1. Nowhere does the Krause Post make any allegation that the In-App Browser uses JavaScript to collect any identifiable information about users' activity on third-party websites for purposes of advertising or sharing with data brokers without user consent. To the contrary, Krause acknowledges unequivocally: "Meta is following the ATT (App Tracking Transparency) rules." Ex. 1 at 3. Krause explains that the post mentions the ATT policy only "to provide some context on why getting data from third party websites/apps is a big deal," given "what is *possible* on a technical level." *Id.* (emphasis added).

The Krause Post includes similar caveats when it goes into more technical detail. Krause focuses in particular on a JavaScript file used by the In-App Browser with the name "pcm.js," which he describes as "code to build a bridge to communicate with the host app." *Id.* Krause expressly includes a "disclaimer" that he does not know what data this code communicates from the In-App Browser to the Facebook or Instagram app, stating: "I don't have a list of precise data Instagram sends back home." *Id.* at 4. He acknowledges, without disputing, an explanation received from Meta that the "pcm.js" code actually "helps Meta respect the user's ATT opt out choice," as it "helps aggregate [i.e., de-identify] events, i.e. online purchase, before those events are used for targeted advertising and measurement for the Facebook platform." *Id.* at 12.

Besides the "pcm.js" code, Krause also states that he identified "additional" JavaScript code related to "tracking the user's text selections"—i.e., actions by a user to select text on a web page with the cursor. *Id.* at 4. Again, however, Krause does not claim to know what this code is actually used for, and he certainly makes no allegation that this code is used to do anything in violation of Apple's ATT policy. Instead, he acknowledges, without disputing, Meta's explanation that the code was originally designed to "allow users to share selected text to their news feed" on Facebook, but that it is "old code that isn't used anymore." *Id.* at 13.

In short, while the Krause Post expresses a generalized concern that customized in-app browsers theoretically *could* be used to collect data for improper purposes, it does not conclude that the In-App Browser on Facebook or Instagram is *actually* used to do so. In fact, it states the opposite and specifically affirms that Meta is complying with Apple's ATT policy.

B. The Rush to File Complaints Against Meta in the Wake of the Krause Post

Shortly after the publication of the Krause Post, the first of several putative class actions was filed in this Court on September 15, 2022, by plaintiff Wayne Mitchell. *See* Dkt. 1 ("*Mitchell* Complaint"). The *Mitchell* Complaint relied on the Krause Post to allege—contrary to Krause's express disclaimers—that Meta was *actually* using the In-App Browser to extensively track Facebook users' activity on third-party websites, allegedly in violation of Apple's ATT policy. The complaint erroneously paraphrased Krause as asserting that, "by running custom scripts on third-party websites, Meta can *and does* intercept, view, monitor, and record all user interactions

[with external websites]—every button and link they tap, as well as text selections, screenshots, form inputs (including passwords, addresses, and payment card numbers), other personally identifiable information, protected health details, and other private and confidential communications and data." Dkt. 1 ¶ 30 (emphasis added). The *Mitchell* Complaint cited no basis for these allegations other than the Krause Post.

After the *Mitchell* Complaint was filed, a slew of copycat complaints were filed in the names of other plaintiffs. In November 2022, the Court consolidated those actions with Mitchell's, Dkts. 21, 25, and shortly thereafter, on December 22, 2022, the Court appointed Mitchell, along with Gabriele Willis and Kerreisha Davis, as Lead Plaintiffs, and named interim class counsel. Dkt. 33. On February 6, 2023, a new group of Plaintiffs filed the Consolidated Class Action Complaint. Dkt. 36.[5]

C. The Consolidated Class Action Complaint

Although Plaintiffs had more than two months after the consolidation order (and nearly six months since the publication of the Krause Post) to independently investigate and substantiate their claims, Plaintiffs added almost no new factual allegations to the Complaint. Instead, they focused on adding plaintiffs from eight different states (in particular, states with wiretapping laws that include statutory damages provisions), and tacking on numerous additional claims to the same flawed factual foundation underlying the previously filed complaints. Plaintiffs now bring 14 claims, alleging violations of the (1) Wiretap Act, 18 U.S.C § 2510 *et seq.*; (2) Computer Fraud and Abuse Act, 18 U.S.C § 1030 *et seq.* ("CFAA"); (3) California Invasion of Privacy Act, Cal. Penal Code § 630 *et seq.*; (4) California Unfair Competition Law, Cal. Bus. & Prof Code § 17200 *et seq.* ("UCL"); (5) Florida Security of Communications Act, Fla. Stat. Ann. § 934.01 *et seq.*; (6) Illinois Eavesdropping Act, 720 ILCS 5/14-1 *et seq.*; (7) Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. State and Cons. State Ann. § 5701 *et seq.*; (8) Washington Privacy Act, Wash. Rev. Code Ann. § 9.73.030; (9) Missouri Wiretap Act, Mo. Stat.

[5] The Plaintiffs named in the now-operative Complaint are: Gabriele Willis, Shelby Cooper, Rama Kolesnikow, Lisa Bush, David Alzate, Mark Letoski, Louis Green, Ed Rennie, Teia Pittman, Raven Johnson, Chanel Robinson, Kevin Zenstein, Mary Thew, and Lisa Evans. Compl. ¶¶ 13-54. Two of the Lead Plaintiffs (Mitchell and Davis) have been dropped from the Complaint.

§ 542.400 *et seq.*; (10) Massachusetts Wiretap Statute, Mass. Gen. Laws Ann. 272 § 99; and (11) Maryland Wiretap Act, Md. Cts. & Jud. Pro. § 10-401 *et seq.*; as well as common-law claims for (12) intrusion upon seclusion; (13) publication of private facts; and (14) unjust enrichment. Compl. ¶¶ 115-316.

The factual allegations underlying Plaintiffs' claims are functionally identical to those in the original *Mitchell* Complaint: in essence, Plaintiffs double-down on their flawed reading of the Krause Post. Citing the Krause Post throughout their description of the functioning of the In-App Browser, Plaintiffs allege that, "[b]y injecting code into third-party websites, Meta is able to track users and intercept data that would otherwise be unavailable to it." *Id.* ¶ 81. Specifically singling out the "pcm.js" code mentioned in the Krause Post, Plaintiffs allege that it is used to collect data for this purpose:

> When the Facebook app injects Meta's JavaScript code ("pcm.js") into a third-party website accessed from within Facebook's in-app browser, it creates a bridge to communicate between the Facebook app and the third-party website. This allows Meta to intercept and record users' interactions and communications with third parties, providing data that Meta analyzes and uses to boost its advertising revenue.

Id. ¶ 86. The Complaint describes the allegedly collected data in sweeping terms, asserting that the JavaScript used by the In-App Browser works like a "keystroke logger" that Meta uses to

> intercept, view, monitor, and record all user interactions with third parties—every button and link users tap, text selections, screenshots, form inputs (including passwords, addresses, and payment card numbers), personally identifiable information, protected health details, and other private and confidential communications and data.

Id. ¶ 89; *see also id.* ¶¶ 93-94, 186, 201, 215, 229, 248, 270, 292.

Plaintiffs further claim that Meta tracks data for "users of iOS 14.5 or later" who "*declined* to consent" to tracking under the ATT policy, *id.* ¶ 95 (emphasis in original)—as Plaintiffs claim they declined, *id.* ¶¶ 13-54—and that Meta did so intentionally in order to use the data for advertising-related purposes in violation of the ATT policy. *Id.* ¶¶ 74, 80. Indeed, they describe the In-App Browser broadly as a "technical workaround" that Meta "devised" in order to "track

its users' activity and communications on third-party websites opened via the Facebook app, even where users expressed their preference not to be tracked on their Apple Device." *Id.* ¶ 5.

The only basis Plaintiffs assert for their claims about the workings of the In-App Browser is the Krause Post. They do not allege that they have done any independent examination or testing of the In-App Browser that is the source of their allegations.

III. LEGAL STANDARDS

Rule 12(b)(1): "To establish Article III standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" *Clapper v. Amensty Int'l USA*, 568 U.S. 398, 409 (2013) (citation omitted). It is not sufficient for a plaintiff to "merely speculate and make assumptions" that a defendant is behaving in harmful ways. *Id.* at 411, 414. Rather, an injury must be "certainly impending" to provide a basis for standing, *id.* at 401, and in a suit for damages in particular, "the mere risk of future harm, standing alone, cannot qualify as a concrete harm." *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2210-11 (2021).

Rule 12(b)(6): A claim must be dismissed unless it pleads "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citation omitted); *see* Fed. R. Civ. P. 12(b)(6). At a minimum, a plaintiff must allege facts sufficient to "raise a right to relief above the speculative level," *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007), and "include sufficient 'factual enhancement' to cross 'the line between possibility and plausibility,'" *Eclectic Props. E., LLC v. Marcus & Millichap Co.*, 751 F.3d 990, 996 (9th Cir. 2014) (quoting *Twombly*, 550 U.S. at 556-57). The Court need not "accept as true allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) (citation omitted).

In addition, under the doctrine of incorporation by reference, a court evaluating a Rule 12(b)(6) motion may consider a document outside of the complaint where the complaint references the document or where it "forms the basis" of Plaintiffs' claims. *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1002-03 (9th Cir. 2018) (citation omitted). Once a document is incorporated

by reference, it is treated as "part of the complaint itself," and the court should assume the document's "contents are true for purposes of a motion to dismiss." *Id.*; *see Knievel v. ESPN*, 393 F.3d 1068, 1076-77 (9th Cir. 2005) (recognizing incorporation by reference doctrine "applies with equal force to internet pages as it does to printed material"). Accordingly, a court "need not credit as true allegations in the complaint that are contradicted by" incorporated documents. *Coyoy v. City of Eloy*, 859 F. App'x 96 (9th Cir. 2021); *see also In re Finjan Holdings, Inc. Secs. Litig.*, 58 F.4th 1048, 1052 n.1 (9th Cir. 2023) ("When a general conclusion in a complaint contradicts specific facts retold in a document . . . incorporated by reference in the complaint . . . those specific facts are controlling."). This "prevents plaintiffs from selecting only portions of documents that support their claims, while omitting portions of those very documents that weaken—or doom—their claims." *Khoja*, 899 F.3d at 1002.

IV. ARGUMENT

A. The Complaint Fails to Plausibly Plead Any Basis for Standing or Any Cause of Action Because the Krause Post Contradicts Plaintiffs' Core Allegations

Plaintiffs' complaint ultimately rests on sheer speculation and surmise rather than any plausibly alleged facts. The only factual basis they assert for their core allegations—i.e., the allegations that Meta collects data on every interaction a user has with a third-party website in the In-App Browser, and uses this data for advertising purposes in violation of Apple's ATT policy—is the Krause Post itself. Yet, the Krause Post contradicts those very allegations. Under the incorporation by reference doctrine, the Court need not and should not credit those contradicted allegations as true. Once those allegations fall away, nothing remains in the Complaint except Plaintiffs' own conjecture about how the In-App Browser works and what Meta uses it for. The Complaint therefore fails to allege a sufficient basis for standing and otherwise fails to "raise a right to relief above the speculative level" for purposes of Rule 8 and Rule 12(b)(6). *Twombly*, 550 U.S. at 555. The entire case should be dismissed for these reasons.

1. The Complaint Incorporates the Krause Post by Reference

There can be no question that the Krause Post is incorporated by reference into the Complaint. A document is incorporated by reference "if the plaintiff refers extensively to the

document or the document forms the basis of the plaintiff's claim." *Khoja*, 899 F.3d at 1002 (citation omitted); *see also Davis v. HSBC Bank Nev., N.A.*, 691 F.3d 1152, 1160-61 (9th Cir. 2012) (district court properly incorporated by reference documents that were referenced in, but not attached to the complaint). Here, either standard is met, as Plaintiffs both "refer[] extensively" to the Krause Post and use it as "the basis of" their claims. *Khoja*, 899 F.3d at 1002 (citation omitted).

First, Plaintiffs make extensive references to the Krause Post in the Complaint, both directly and indirectly. They cite the Krause Post expressly at the outset of section E of the Complaint—which contains their core factual allegations about the operations of the In-App Browser. Compl. ¶¶ 82-84. The paragraphs that follow in the section repeatedly reference concepts and terminology described in the Krause Post and are presented as paraphrased versions of Krause's conclusions. *Id.* ¶¶ 85-96. One of the paragraphs in particular includes a large block quote taken directly from the Krause Post. *Id.* ¶ 94. Plaintiffs also copy and incorporate multiple graphics from the Krause Post. *Compare* Compl. ¶ 82 (Figure 2) *with* Ex. 1 at 7, *and* Compl. ¶ 86 (Figure 4) *with* Ex. 1 at 8. Because Plaintiffs extensively refer to, quote, summarize, and copy portions of the Krause Post in the Complaint, it is properly considered incorporated. *See Khoja*, 899 F.3d at 1003-04 (blog post held to be incorporated by reference where plaintiff "did more than merely mention it," and included a "lengthy" quote that "convey[ed] numerous facts"); *In re Eventbrite, Inc. Sec. Litig.*, No. 5:18-CV-02019-EJD, 2020 WL 2042078, at *7 (N.D. Cal. Apr. 28, 2020) (incorporating documents where "Plaintiffs explicitly and repeatedly refer[red] to excerpts of these exhibits to support their claims").

Second, the Krause Post also forms the basis for Plaintiffs' claims. Plaintiffs specifically cite the Krause Post as the putative source of their allegations concerning how the IAW works and what Meta does with it, stating that: "Krause's report . . . describes how Meta uses JavaScript to alter websites and override its users' default privacy settings," Compl. ¶ 84; and "Krause further describe[s] technical elements of [the] process" by which Meta is purportedly "able to surveil and extract details about users' texting, selections, and other communications with third-party websites," Compl. ¶ 94. Even more tellingly, Plaintiffs do not cite anything else *besides* the Krause Post as the source for their allegations about the IAW: they do not cite findings by any other

researcher, nor do they claim to have engaged any expert themselves to conduct independent testing of the IAW. Because Plaintiffs plainly rely on the Krause Post as the factual basis for their claims—the Complaint would not have been filed without it—it is incorporated by reference for this reason as well. *See Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 679 n.1 (N.D. Cal. 2021) (finding that media article about alleged privacy issue that prompted plaintiffs to bring suit was "the basis of Plaintiffs' claims" and was therefore incorporated by reference).

Accordingly, under either rationale recognized by *Khoja*, the Krause Post is incorporated by reference into the Complaint and may be considered by the Court in resolving the instant motion.

2. The Krause Post Contradicts Plaintiffs' Core Allegations

The Complaint boils down to two core allegations, both of which putatively rely on the Krause Post: (1) the allegation that Meta monitors and records every action users take in the In-App Browser, capturing everything from passwords to health information and everything in between; and (2) the allegation that Meta does so in circumvention of Apple's ATT policy. These allegations animate all of Plaintiffs' causes of action (each of which asserts in one way or another that their communications with third-party websites were collected without their consent)[6] as well as their theory of harm.[7]

Both of these allegations, however, are contradicted by the Krause Post. As to the allegation that Meta monitors and records every action users take in the In-App Browser, the Krause Post specifically disavows that very claim. While Krause expresses concern that a custom

---

[6] *See* Compl. ¶ 122 (alleging Wiretap Act violation because "Meta intercepted the contents of their electronic communications"); *id.* ¶ 141 (alleging CFAA violation because Plaintiffs "did not consent to be tracked by the Facebook app across third-party websites"); *id.* ¶ 154 (alleging CIPA violation because "Meta failed to disclose that it was intercepting, tracking and learning the contents of such private conversations and activities"); *id.* ¶ 168 (alleging UCL violation because "Meta actively intercepted, viewed, and collected" user information); *id.* ¶¶ 188, 203, 216, 230, 250, 272, 294 (alleging state law violations because "Meta intentionally intercepted" Plaintiffs' information); *id.* ¶ 301 (alleging intrusion upon seclusion because "Meta monitored, intercepted, transmitted and recorded" Plaintiffs' information); *id.* ¶ 308 (alleging publication of private facts based on "Meta's surreptitious tracking"); *id.* ¶ 311 (alleging unjust enrichment because "Meta secretly intercepts, monitors, and records").

[7] *See* Compl. ¶ 101 (alleging privacy harm on the basis that "Plaintiffs reasonably believed that their communications and interactions with third-party websites were solely with those sites").

in-app browser *could* be used by an app developer in this way, he repeatedly caveats that Meta does *not actually* do so with the In-App Browser. Ex. 1 at 1-3. Krause makes clear that he does not know what data Meta is actually collecting (if any) through the In-App Browser, and he expressly disclaims wild-eyed allegations of the sort that Plaintiffs make, to the effect that Meta captures anything and everything that users do in the In-App Browser, no matter how sensitive. *See id.* Plaintiffs ignore this contradictory information—even where Krause repudiates statements phrased in almost the exact wording that Plaintiffs use:

Krause Post	**Plaintiffs' Complaint**
"*Even though the injected script doesn't currently do this*, running custom scripts on third party websites allows them to monitor all user interactions, like every button & link tapped, text selections, screenshots, as well as any form inputs, like passwords, addresses and credit card numbers." Ex. 1 at 1-2 (emphasis added).	"These event listeners [*i.e.*, injected JavaScript] are critical to Meta's ability to intercept, view, monitor, and record all user interactions with third parties—every button and link users tap, text selections, screenshots, form inputs (including passwords, addresses, and payment card numbers), personally identifiable information, protected health details, and other private and confidential communications and data." Compl. ¶ 89.
"'Does Facebook *actually* steal my passwords, address and credit card numbers?' No! I didn't prove the exact data Instagram is tracking, but wanted to showcase the kind of data they *could* get without you knowing." Ex. 1 at 3 (emphasis added).	"In the context of an online purchase, Facebook's in-app browser collects and records all details of the purchase, including the item purchased; name and address of purchaser; their telephone number, credit card or bank information, usernames, passwords and birthdate; and the purchase price." Compl. ¶ 89.

Likewise, as to whether Meta uses the In-App Browser to circumvent the ATT policy, the Krause Post rejects that claim unequivocally, stating that "Meta is following the ATT (App Tracking Transparency) rules." Ex. 1 at 3. That statement plainly means that Meta is *not* "tracking" users through the In-App Browser when they have opted-out of "tracking" on their

Apple devices. Indeed, Krause acknowledges, without disputing, Meta's statement that the "pcm.js" JavaScript code that he identifies is specifically designed to help *comply* with the ATT policy. *Id.* at 12-13. Thus, Plaintiffs' allegation that Meta is collecting information about them in violation of the ATT policy—which is critical to the alleged lack of consent that runs through all of their claims—is specifically contradicted by the Krause Post.

Because Plaintiffs' allegations are specifically contradicted by the document they rely on as the basis for those allegations—indeed, as the basis for their Complaint overall—the Court need not and should not credit those allegations. Plaintiffs are not entitled to invent their own facts. If the Krause Post is the putative factual basis for their lawsuit, then they are not entitled to disregard the limitations of what it says. That is precisely why the doctrine of incorporation by reference exists—to prevent Plaintiffs from "selecting only portions of a document that support their claims, while omitting portions . . . that weaken—or doom—their claims." *Khoja*, 899 F.3d at 1002-03 (9th Cir. 2018). Therefore a court "need not accept as true conclusory allegations that are contradicted by documents referred to in the complaint." *Tritz v. U.S. Postal Serv.*, 721 F.3d 1133, 1135 n.1 (9th Cir. 2013).

Lopez provides an instructive example of a court finding an article on the internet to be incorporated into a complaint by reference and declining to credit conclusory statements in the complaint that are contradicted by it. 519 F. Supp. 3d at 680-82. There, the plaintiffs' complaint alleged "in a conclusory fashion[] that their communications were intercepted" by Apple through the Siri assistant on their iPhones, but "the complaint ma[de] clear that their allegations [were] based entirely on [a] Guardian [newspaper] article." *Id.* at 681. The court closely reviewed the article (which the court *sua sponte* found had been incorporated by reference, *id.* at 679 n.1) and held that it did not lend plausible support to their allegations. In particular, the court found that it "does not plausibly suggest that all Apple's devices were subject to accidental triggers" that supposedly caused Siri to intercept users' private information, much less that plaintiffs' "own private communications were intercepted by accidental triggers." *Id*. at 681. Thus, the court set aside the conclusory allegations made by the plaintiffs in the complaint and instead decided the case on a motion to dismiss based on what the relied-upon news article actually said, as opposed

to the plaintiffs' overreading of it. *Id.* at 680-82 (finding that plaintiff lacked standing for intrusion upon seclusion, Wiretap Act, and CIPA claims that were based on the article); *see also In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 816-17 (N.D. Cal. 2020) (rejecting wiretapping allegations based on a third party-report where the report did not imply that the plaintiffs' own conversations had been intercepted).

A similar approach should be followed here. Plaintiffs' allegations that Meta *actually* uses JavaScript in the In-App Browser to monitor and record all user browsing activity in an effort to circumvent Apple's ATT policy are conclusory taken on their own and are contradicted by the Krause Post. Accordingly, the allegations should not be accepted as true. With those contradicted allegations removed, Plaintiffs are left only with the Krause Post's generalized concern that a custom in-app browser *could* be used to monitor everything a user does, or Plaintiffs' own speculation that Meta *could* be doing so through the In-App Browser. But of course the mere *possibility* of improper conduct is insufficient to establish Plaintiffs' standing to sue. *See Clapper*, 568 U.S. at 414 (rejecting standing where plaintiffs could only conjecture they were being unlawfully surveilled and had no evidence that such surveillance was actually occurring). Once Plaintiffs' distorted portrayal of the Krause Post is excised from the Complaint, that mere possibility of harm is all they can allege, which does not provide a viable foothold for standing with respect to any of their causes of action. *See Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1188 (N.D. Cal. 2020) (finding no Article III standing for wiretapping and privacy claims where complaint "did little more than parrot internet musings about things Facebook may or may not be doing" and there was no basis to infer plaintiffs had actually suffered any privacy harm "[w]hen these fillers [we]re stripped away"); *see also TransUnion*, 141 S. Ct. at 2212 (finding the mere risk that plaintiffs' private information would be divulged "too speculative to support Article III standing").

Likewise, the mere possibility of alleged non-consensual "interception" of communications, standing alone, is insufficient as a matter of law to sustain a "facially plausible" claim for relief on any of the violations alleged in the Complaint. *See Iqbal*, 556 U.S. at 678-79 (explaining that the alleged facts must "permit the court to infer more than the mere possibility of

misconduct" to survive a motion to dismiss). Each of the alleged causes of action depends on Meta having *actually* collected Plaintiffs' data without their consent. Because the Krause Post contradicts Plaintiffs' core allegations to that effect, none of their causes of action has any plausible factual basis. *See In re Finjan Holdings, Inc. Secs. Litig.*, No. 20-cv-04289, 2021 WL 4148682, at *3 (N.D. Cal. Sep. 13, 2021) (rejecting allegations based on "selective[] cites" where plaintiff "ignore[d] those parts of the document that do not favor him, precisely what *Khoja* says a plaintiff may not do"), *aff'd*, 58 F.4th 1048 (9th Cir. 2023); *Alamilla v. Hain Celestial Grp., Inc.*, 30 F. Supp. 3d 943, 944 (N.D. Cal. 2014) (dismissing complaint based on articles incorporated by reference in the complaint, where "[t]he articles the plaintiffs cite . . . contradict the allegation upon which their entire complaint hinges").

Accordingly, upon finding the Krause Post to be incorporated by reference, the Court should dismiss the Complaint in its entirety, for lack of standing and for failure to state a claim.

B. Plaintiffs' CFAA and Equitable Claims Fail for Additional, Claim-Specific Reasons

While the Court need not address any of Plaintiffs' specific claims given their lack of a plausible factual basis for the Complaint as a whole, their CFAA claims and their equitable claims independently fail due to claim-specific legal defects.

1. Plaintiffs' CFAA Claim Fails Because They Do Not Allege Conduct Constituting Computer Hacking or Any Cognizable Damage or Loss

Plaintiffs' CFAA claim fails as a matter of law because Plaintiffs do not allege conduct constituting computer hacking. "The CFAA was enacted to prevent intentional intrusion onto someone else's computer—specifically, computer hacking." *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1196 (9th Cir. 2022). The conduct prohibited is meant to be "analogous to 'breaking and entering.'" *Id.* (quoting H.R. Rep. No. 98-894, at 20 (1984)). Plaintiffs do not (and cannot) allege any such conduct. They allege that Meta collected information from the Plaintiffs through the In-App Browser—which, as Plaintiffs themselves allege, is "on Facebook's own platform," i.e., is part of Meta's own app. Compl. ¶ 5; *see also id.* ¶ 81 (stating that when Meta "reroutes the user to its own in-app web browser," "[t]hird party websites are rendered *inside* the app" (emphasis

in original)). Obviously, Meta cannot be said to have hacked into its own app; nor can Meta be said to have hacked into the part of Plaintiffs' mobile devices where the app resides, as Plaintiffs voluntarily downloaded the app onto their devices. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1065-69 (N.D. Cal. 2012) (stating that, where "software or 'apps' that allegedly harmed the phone were voluntarily downloaded by the user, other courts . . . have reasoned that users would have serious difficulty pleading a CFAA violation").

Plaintiffs try to stretch the CFAA to apply here by invoking its prohibition on "exceeding authorized access" to a computer, arguing that Meta exceeded authorized access to their devices by collecting data about their browsing activity even though they had opted out of "tracking" through Apple's ATT mechanism. *See* Compl. ¶ 141. But, as the Supreme Court has made clear, the CFAA's "exceeds authorized access" provision is not implicated by the alleged *misuse* of access that a defendant has to a computer; it still requires some part of the computer to be *hacked*. *See Van Buren v. United States*, 141 S. Ct. 1648, 1658–59 (2021) (holding that the CFAA's "access without authorization" prong and its "exceeds authorized access" prong both require "a gates-up-or-down inquiry" as to whether the defendant breached a barrier to access). Thus, in *Van Buren*, the Supreme Court found that a defendant police officer could not be charged under the CFAA's "exceeds authorized access" provision based on his misuse of a law enforcement database to look up information about individuals for improper purposes, even though the searches were in violation of department policy. *Id.* at 1648, 1653, 1658-62. Instead, the Court construed the provision narrowly, so as to apply only when someone "accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off limits to him." *Id.* at 1662; *see also United States v. Nosal*, 676 F.3d 854, 862 (9th Cir. 2012) (en banc) (rejecting argument that "exceeds authorized access" prong extends to conduct "in violation of computer use restrictions," finding that it would "transform the CFAA from an anti-hacking statute into an expansive misappropriation statute").

Similarly, here, any allegation that Meta collected data from Plaintiffs in violation of the ATT policy does not provide a basis for a claim that Meta "exceeded authorized access" under the CFAA. Regardless of the alleged impropriety of such data collection, it does not involve accessing

an area of a computer "off limits" to Meta. To the contrary, the alleged conduct took place in Meta's own app, not some "off limits" location outside the app. *See Ji v. Naver Corp.*, No. 21-cv-05143-HSG, 2022 WL 4624898, at *11 (N.D. Cal. Sept. 30, 2022) (rejecting CFAA claim based on app developer's alleged collection of facial data from app without user's consent, given that "data collection and device hacking are distinct" and that "only the latter is at issue in a CFAA claim" (internal quotation marks and citation omitted)).

Additionally, Plaintiffs' CFAA claim fails because Plaintiffs do not allege any "damage or loss" that is recoverable under the CFAA. The CFAA's civil remedy provision only allows suit by a person who, *inter alia*, "suffers damage or loss by reason of a violation" of the statute. 18 U.S.C. § 1030(g). The term "damage" is defined to refer to the "impairment to the integrity or availability of data, a program, a system, or information," *id.* § 1030(e)(8), while the term "loss" is defined to refer to any "reasonable cost" of the conduct to the victim, such as the cost of "conducting a damage assessment" or "consequential damages incurred because of the interruption of service," *id.* § 1030(e)(11). Plaintiffs allege no such "damage" or "cost" here. Instead, Plaintiffs allege that Meta "decreas[ed] the value of their private and personally identifiable information and communications" and "imped[ed] their ability to control the dissemination and use of such information and communications." Compl. ¶ 146. Allegations of this nature are far afield from what the statutory terms encompass. *See Van Buren*, 141 S. Ct. at 1660 (finding the definitions of "loss" and "damage" "ill fitted . . . to remediating 'misuse' of sensitive information"); *Andrews v. Sirius XM Radio Inc.*, 932 F. 3d 1253, 1262-63 (9th Cir. 2019) (finding the "loss" definition did not cover alleged loss of value of personal data).

Moreover, in addition to requiring "loss" or "damage," the CFAA's civil remedy section also requires at least one of several aggravating harm factors to exist, none of which Plaintiffs adequately allege here. *See* 18 U.S.C. § 1030(g) (cross-referencing factors set forth in § 1030(c)(4)(A)(i)). In particular, Plaintiffs do not allege facts sufficient to show "loss" aggregating at least $5,000 in value, *see id.* § 1030(c)(4)(A)(i)(I) (cited at Compl. ¶ 145), because they do not allege any "loss" as defined in the statute at all. And to the extent that Plaintiffs rely on an alleged "threat to public health and safety," Compl. ¶ 147 (citing 18 U.S.C.

§ 1030(c)(4)(A)(i)(IV)), they have not pled any facts to support that conclusion, which is absurd on its face.

For all of these reasons, Plaintiffs' CFAA claim must be dismissed.

2. Plaintiffs' Claims for Equitable Relief Fail Because They Cannot Allege They Lack an Adequate Remedy at Law

Plaintiffs' claims under the UCL (Claim 4), unjust enrichment (Claim 14), and their more general request for equitable relief (Prayer for Relief ¶ D) should be dismissed because Plaintiffs do not plead that they lack an adequate remedy at law. *See Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844-45 (9th Cir. 2020). In *Sonner*, the Ninth Circuit held that plaintiffs seeking equitable relief in federal court must plausibly plead that they "lack[] an adequate legal remedy." *Id.* at 844. The Ninth Circuit has since reaffirmed *Sonner*, and courts in this district have repeatedly followed it. *See e.g., Guzman v. Polaris Indus. Inc.*, 49 F.4th 1308, 1313-15 (9th Cir. 2022) (holding that the "district court lacked equitable jurisdiction to hear" UCL claim given that plaintiff had "an adequate legal remedy"); *Klaehn v. Cali Bamboo LLC*, No. 21-55738, 2022 WL 1830685, at *3 (9th Cir. June 3, 2022) (affirming dismissal of UCL claim where "Plaintiffs failed to make any plausible allegation that they lacked an adequate remedy at law"); *see also Smith v. Apple, Inc.*, No. 21-cv-09527-HSG, 2023 WL 2095914, at *3 (N.D. Cal. Feb. 17, 2023) (plaintiff cannot "plead[] equitable remedies in the alternative" if a plaintiff has not plausibly alleged that their remedies at law are inadequate); *Price v. Apple, Inc.*, No. 21-cv-02846-HSG, 2022 WL 1032472, at *7 (N.D. Cal. Apr. 6, 2022) (dismissing with prejudice claims for equitable relief because claims could be adequately remedied with money damages).

Here, Plaintiffs seek statutory and punitive damages under the Wiretap Act and state equivalents, "economic damages" under the CFAA, and "monetary damages" for their common law privacy claims. Compl. ¶¶ 129, 148, 159-60, 190-91, 205, 218, 233, 252-53, 274-75, 296-97, 303, 310. Plaintiffs have not alleged that any of these legal remedies are "inadequate." Rather, Plaintiffs make conclusory allegations that they "lack an adequate remedy at law," *id.* ¶¶ 175, 312, but fail to provide any substantive allegations supporting that conclusion. Such allegations are insufficient to support a claim for equitable relief, including requests for injunctive relief and

restitution. *In re ZF-TRW Airbag Control Units Prod. Liab. Litig.*, 601 F. Supp. 3d 625, 768-70 (C.D. Cal. 2022); *Reilly v. Apple Inc.*, 578 F. Supp. 3d 1098, 1112-13 (N.D. Cal. 2022) (dismissing claims for injunctive relief and restitution where plaintiff "merely assert[ed] that he lack[ed] adequate remedies at law, but fail[ed] to allege facts or reasons why that is the case" (citation omitted)). Indeed, Plaintiffs not only do not but *cannot* show that their legal remedies are inadequate, because the claims on which they seek to recover damages arise from the "exact same conduct" as their pled equitable claims. *Price*, 2022 WL 1032472, at *7. All of Plaintiffs' equitable claims are thus defective—incurably so—and must be dismissed.

3. Plaintiffs' UCL Claim Additionally Fails Because They Do Not Allege an Economic Injury

In addition to being subject to dismissal under *Sonner*, Plaintiffs' UCL claim is separately subject to dismissal because Plaintiffs fail to allege an economic injury. The UCL limits statutory standing to those who have "suffered injury in fact and ha[ve] lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204; *Birdsong v. Apple, Inc.*, 590 F.3d 955, 959-60 (9th Cir. 2009). None of Plaintiffs' allegations is sufficient to show that they suffered any such loss. Their sole allegation on this front is that their "loss of their personal information constitutes an economic injury" because they have a "property right in their personal information." Compl. ¶ 175. But California courts have rejected the notion that a "lost-value-of-PII theory" is sufficient to demonstrate loss of money or property. *Moore v. Centrelake Med. Grp., Inc.*, 83 Cal. App. 5th 515, 538 (2022); *see also Gardiner v. Walmart, Inc.,* No. 20-CV-04618-JSW, 2021 WL 2520103, at *8 (N.D. Cal. Mar. 5, 2021) ("Courts have widely held that 'personal information' does not constitute [such lost] money or property under the UCL."); *Rodriguez v. Google LLC*, No. 20-cv-04688-RS, 2021WL 2026726, at *8 (N.D. Cal. May 21, 2021) (individual digital data is not considered "money or property"); *Wesch v. Yodlee, Inc.*, 20-cv-05991-SK, 2021 WL 6206644, at *4 (N.D. Cal. July 19, 2021) (dismissing UCL claim based on lack of a "current market for individuals to sell their financial data"); *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1040 (N.D. Cal. 2019) ("That the information has external value, but no economic value to plaintiff,

cannot serve to establish that plaintiff has personally lost money or property."). Accordingly, Plaintiffs' UCL claim must be dismissed for this reason as well.

V. CONCLUSION

For the foregoing reasons, Meta respectfully requests that this action be dismissed in its entirety, without leave to amend.[8]

Dated: March 23, 2023

LATHAM & WATKINS LLP

By: */s/ Serrin Turner*

Elizabeth L. Deeley (Bar No. 230798)
elizabeth.deeley@lw.com
Sheridan Caldwell (Bar No. 324743)
sheridan.caldwell@lw.com
505 Montgomery Street, Suite 2000
San Francisco, CA 94111-6538
Telephone: +1.415.391.0600

Serrin Turner (*pro hac vice*)
serrin.turner@lw.com
Marissa Alter-Nelson (*pro hac vice*)
marissa.alter-nelson@lw.com
1271 Avenue of the Americas
New York, New York 10022-4834
Telephone: +1.212.906.1200

Attorneys for Defendant Meta Platforms, Inc.

[8] *See Gershfeld v. Teamviewer US, Inc.*, No. 21-55753, 2023 WL 334015, at *2 (9th Cir. Jan. 20, 2023) (affirming denial of leave to amend because "complaint could not be saved by amendment" where it was based on incorrect facts, as demonstrated by incorporated document).